

# COMPUTING THE MAZUR AND SWINNERTON-DYER CRITICAL SUBGROUP OF ELLIPTIC CURVES

HAO CHEN

**ABSTRACT.** Let  $E$  be an optimal elliptic curve defined over  $\mathbb{Q}$ . The *critical subgroup* of  $E$  is defined by Mazur and Swinnerton-Dyer as the subgroup of  $E(\mathbb{Q})$  generated by traces of branch points under a modular parametrization of  $E$ . We prove that for all rank two elliptic curves with conductor smaller than 1000, the critical subgroup is torsion. First, we define a family of *critical polynomials* attached to  $E$  and describe two algorithms to compute such polynomials. We then give a sufficient condition for the critical subgroup to be torsion in terms of the factorization of critical polynomials. Finally, a table of critical polynomials is obtained for all elliptic curves of rank two and conductor smaller than 1000, from which we deduce our result.

## 1. INTRODUCTION

**1.1. Preliminaries.** Let  $E$  be an elliptic curve over  $\mathbb{Q}$  and let  $L(E, s)$  be the  $L$ -function of  $E$ . The rank part of the Birch and Swinnerton-Dyer (BSD) conjecture states that

$$\text{rank}(E(\mathbb{Q})) = \text{ord}_{s=1} L(E, s).$$

The right hand side is called the *analytic rank* of  $E$ , and is denoted by  $r_{\text{an}}(E)$ . The left hand side is called the *algebraic rank* of  $E$ . The rank part of the BSD conjecture is still open when  $r_{\text{an}}(E) > 1$ , and its proof for  $r_{\text{an}}(E) = 1$  uses the *Gross-Zagier formula*, which relates the value of certain  $L$ -functions to heights of Heegner points.

Let  $N$  be the conductor of  $E$ . The modular curve  $X_0(N)$  is a nonsingular projective curve defined over  $\mathbb{Q}$ . Since  $E$  is modular (Breuil, Conrad, Diamond, and Taylor [2]), there is a surjective morphism  $\varphi : X_0(N) \rightarrow E$  defined over  $\mathbb{Q}$ . Let  $\omega_E$  be the invariant differential on  $E$  and let  $\omega = \varphi^*(\omega_E)$ . Then  $\omega$  is a holomorphic differential on  $X_0(N)$  and we have  $\omega = cf(z)dz$ , where  $f$  is the normalized newform attached to  $E$  and  $c$  is a nonzero constant. In the rest of the paper, we fix the following notations: the elliptic curve  $E$ , the conductor  $N$ , the morphism  $\varphi$ , and the differential  $\omega$ .

Let  $R_\varphi = \sum_{[z] \in X_0(N)} (e_\varphi(z) - 1)[z]$  be the ramification divisor of  $\varphi$ .

**Definition 1.1** (Mazur and Swinnerton-Dyer [9]). The *critical subgroup* of  $E$  is

$$E_{\text{crit}}(\mathbb{Q}) = \langle \text{tr}(\varphi([z])) : [z] \in \text{supp } R_\varphi \rangle,$$

where  $\text{tr}(P) = \sum_{\sigma: \mathbb{Q}(P) \rightarrow \mathbb{Q}} P^\sigma$ .

Since the divisor  $R_\varphi$  is defined over  $\mathbb{Q}$ , every point  $[z]$  in its support is in  $X_0(N)(\overline{\mathbb{Q}})$ , hence  $\varphi([z]) \in E(\overline{\mathbb{Q}})$ , justifying the trace operation. The group  $E_{\text{crit}}(\mathbb{Q})$  is a subgroup of  $E(\mathbb{Q})$ . Observe that  $R_\varphi = \text{div}(\omega)$ , thus  $\deg R_\varphi = 2g(X_0(N)) - 2$ . In the rest of the paper, we use the notation  $\text{div}(\omega)$  in place of the ramification divisor  $R_\varphi$ . In addition, we will assume  $E$  is an optimal elliptic curve, so  $\varphi$  is unique up to sign. This justifies the absence of  $\varphi$  in the notation  $E_{\text{crit}}(\mathbb{Q})$ .

Recall the construction of *Heegner points*: for an imaginary quadratic order  $\mathcal{O} = \mathcal{O}_d$  of discriminant  $d < 0$ , let  $H_d(x)$  denote its *Hilbert class polynomial*.

**Definition 1.2.** A point  $[z] \in X_0(N)$  is a “*generalized Heegner point*” if there exists a negative discriminant  $d$  s.t.  $H_d(j(z)) = H_d(j(Nz)) = 0$ . If in addition we have  $(d, 2N) = 1$ , then  $[z]$  is a *Heegner point*.

For any discriminant  $d$ , let  $E_d$  denote the quadratic twist of  $E$  by  $d$ . Then the Gross-Zagier formula in [7] together with a non-vanishing theorem for  $L(E_d, 1)$  (see, for example, Bump, Friedberg, and Hoffstein [3]) implies the following

**Theorem 1.3.** (1) If  $r_{\text{an}}(E) = 1$ , then there exists a Heegner point  $[z]$  on  $X_0(N)$  such that  $\text{tr}(\varphi([z]))$  has infinite order in  $E(\mathbb{Q})$ .

(2) If  $r_{\text{an}}(E) \geq 2$ , then  $\text{tr}(\varphi([z])) \in E(\mathbb{Q})_{\text{tors}}$  for every “generalized Heegner point”  $[z]$  on  $X_0(N)$ .

The first case in the above theorem is essential to the proof of rank BSD conjecture for  $r_{\text{an}}(E) = 1$ .

Observe that the defining generators of the critical subgroup also take the form  $\text{tr}(\varphi([z]))$ . Then a natural question is:

**Question 1.4.** Does there exist an elliptic curve  $E/\mathbb{Q}$  with  $r_{\text{an}}(E) \geq 2$  and  $\text{rank}(E_{\text{crit}}(\mathbb{Q})) > 0$ ?

We will show that the answer is negative for all elliptic curves with conductor  $N < 1000$ , using *critical polynomials* attached to elliptic curves.

**1.2. Main results.** Let  $E, N, \varphi$ , and  $\omega$  be as defined previously, and write  $\text{div}(\omega) = \sum_{[z] \in X_0(N)} n_z [z]$ . Let  $j$  denote the  $j$ -invariant function.

**Definition 1.5.** The *critical  $j$ -polynomial* of  $E$  is

$$F_{E,j}(x) = \prod_{z \in \text{supp div}(\omega), j(z) \neq \infty} (x - j(z))^{n_z}.$$

Since  $\text{div}(\omega)$  is defined over  $\mathbb{Q}$  and has degree  $2g(X_0(N)) - 2$ , we have  $F_{E,j}(x) \in \mathbb{Q}[x]$  and  $\deg F_{E,j} \leq 2g(X_0(N)) - 2$ , where equality holds if  $\text{div}(\omega)$  does not contain cusps. For any non-constant modular function  $h \in \mathbb{Q}(X_0(N))$ , the *critical  $h$ -polynomial* of  $E$  is defined similarly, by replacing  $j$  with  $h$ .

In this paper we give two algorithms *Poly Relation* and *Poly Relation-YP* to compute critical polynomials. The algorithm *Poly Relation* computes the critical  $j$ -polynomial  $F_{E,j}$ , and the algorithm *Poly Relation* computes the critical  $h$ -polynomial  $F_{E,h}$  for some modular function  $h$ , chosen within the algorithm.

We then relate the critical polynomials to the critical subgroup via the following theorem. Recall that  $H_d(x)$  denotes the Hilbert class polynomial associated to a negative discriminant  $d$ .

**Theorem 1.6.** Suppose  $r_{\text{an}}(E) \geq 2$ , and assume at least one of the following holds:

- (1)  $F_{E,h}$  is irreducible for some non-constant function  $h \in \mathbb{Q}(X_0(N))$ .
- (2) There exists negative discriminants  $D_k$  and positive integers  $s_k$  for  $1 \leq k \leq m$ , satisfying  $\mathbb{Q}(\sqrt{D_k}) \neq \mathbb{Q}(\sqrt{D_{k'}})$  for all  $k \neq k'$ , and an irreducible polynomial  $F_0 \in \mathbb{Q}[x]$ , such that

$$F_{E,j} = \prod_{k=1}^m H_{D_k}^{s_k} \cdot F_0.$$

Then  $\text{rank}(E_{\text{crit}}(\mathbb{Q})) = 0$ .

Combining Theorem 1.6 with our computation of critical polynomials, we verified

**Corollary 1.7.** For all elliptic curves  $E$  of rank 2 and conductor  $N < 1000$ , the rank of  $E_{\text{crit}}(\mathbb{Q})$  is zero.

The paper is organized as follows: in Sections 2 and 3, we describe the algorithms *Poly Relation* and *Poly Relation-YP*. In Section 4, we prove Theorem 1.6. Last, in Section 5, we show a table of critical polynomials for all elliptic curves with rank 2 and conductor smaller than 1000, and prove Corollary 1.7.

## 2. THE ALGORITHM *Poly relation*

Let  $C/\mathbb{Q}$  be a nonsingular projective curve. For a rational function  $r \in \mathbb{Q}(C)$ , let  $\text{div}_0(r)$  denote its divisor of zeros. We then define  $\deg r = \deg(\text{div}_0(r))$ .

**Definition 2.1.** Let  $C/\mathbb{Q}$  be a nonsingular projective curve, and let  $r, u$  be two non-constant rational functions on  $C$ . A *minimal polynomial relation between  $r$  and  $u$*  is an irreducible polynomial  $P(x, y) \in \mathbb{Q}[x, y]$  such that  $P(r, u) = 0$  and  $\deg_x(P) \leq \deg u$ ,  $\deg_y(P) \leq \deg r$ .

Minimal polynomial relation always exists and is unique up to scalar multiplication. Write  $\text{div}(r) = \sum n_z [z]$  and  $P(x, y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$ . We have

**Proposition 2.2.** If  $\mathbb{Q}(C) = \mathbb{Q}(r, u)$  and  $\gcd(f_0(y), f_n(y)) = 1$ , then there is a constant  $c \neq 0$  s.t.

$$f_0(y) = c \prod_{z \in \text{div}_0(r) \setminus \text{div}_\infty(u)} (y - u(z))^{n_z}.$$

*Proof.* Dividing  $P(x, y)$  by  $f_n(y)$ , we get  $x^n + \cdots + \frac{f_0(x)}{f_n(y)}$ , a minimal polynomial of  $r$  over  $\mathbb{Q}(u)$ . So  $\text{Norm}_{\mathbb{Q}(r, u)/\mathbb{Q}(u)}(r) = \frac{f_0(u)}{f_n(u)}$ . The rest of the proof uses a theorem on extensions of valuations (see, for example, [10, Theorem 17.2.2]), which we now quote.

**Theorem 2.3.** *Suppose  $v$  is a nontrivial valuation on a field  $K$  and let  $L$  be a finite extension of  $K$ . Then for any  $a \in L$ ,*

$$\sum_{1 \leq j \leq J} w_j(a) = v(\text{Norm}_{L/K}(a)),$$

where the  $w_j$  are normalized valuations equivalent to extensions of  $v$  to  $L$ .

For any  $z_0 \in C$  such that  $u(z_0) \neq \infty$ , consider the valuation  $v = \text{ord}_{(u-u(z_0))}$  on  $\mathbb{Q}(u)$ . The set of extensions of  $v$  to  $\mathbb{Q}(C) = \mathbb{Q}(r, u)$  is in bijection with  $\{z \in C : u(z) = u(z_0)\}$ . Take  $a = r$  and apply Theorem 2.3, we obtain

$$\sum_{z: u(z)=u(z_0)} \text{ord}_z(r) = \text{ord}_{u-u(z_0)} \frac{f_0(u)}{f_n(u)}.$$

Combining the identities for all  $z_0 \in C \setminus \text{div}_\infty(u)$ , we have

$$\prod_{z \in \text{div}(r): u(z) \neq \infty} (y - u(z))^{n_z} = c \cdot \frac{f_0(y)}{f_n(y)}.$$

If  $r(z) = 0$ , then the condition  $\gcd(f_0(y), f_n(y)) = 1$  implies that  $f_0(u(z)) = 0$  and  $f_n(u(z)) \neq 0$ . Therefore,

$$f_0(y) = c \prod_{z \in \text{div}_0(r) \setminus \text{div}_\infty(u)} (y - u(z))^{n_z}.$$

This completes the proof. □

For completeness we also deal with the case where  $u(z) = \infty$ . The corresponding valuation is  $\text{ord}_\infty(\frac{f}{g}) = \deg g - \deg f$ , and we have

$$\sum_{z: u(z)=\infty} \text{ord}_z(r) = \deg f_n - \deg f_0.$$

We will apply Proposition 2.2 to the computation of  $F_{E,j}$ . Consider  $dj = j'(z)dz$ , viewed as a differential on  $X_0(N)$ . Fix the following two modular functions on  $X_0(N)$ :

$$(1) \quad r = j(j - 1728) \frac{\omega}{dj}, \quad u = \frac{1}{j}.$$

First we compute the divisor of  $r$ . Let  $\mathcal{E}_2(N)$  and  $\mathcal{E}_3(N)$  denote the set of elliptic points of order 2 and 3 on  $X_0(N)$ , respectively. Then

$$(2) \quad \text{div}(dj) = -j^*(\infty) - \sum_{c=\text{cusp}} c + \frac{1}{2} \left( j^*(1728) - \sum_{z \in \mathcal{E}_2(N)} z \right) + \frac{2}{3} \left( j^*(0) - \sum_{z \in \mathcal{E}_3(N)} z \right).$$

Writing  $j^*(\infty) = \sum_{c=\text{cusp}} e_c[c]$ , we obtain

$$(3) \quad \text{div}(r) = \text{div}(\omega) + \frac{1}{2} \left( j^*(1728) + \sum_{z \in \mathcal{E}_2(N)} z \right) + \frac{1}{3} \left( j^*(0) + 2 \sum_{z \in \mathcal{E}_3(N)} z \right) - \sum_{c=\text{cusp}} (e_c - 1)[c].$$

Note that (3) may not be the simplified form of  $\text{div}(r)$ , due to possible cancellations when  $\text{supp div}(\omega)$  contains cusps. But since the definition of  $F_{E,j}$  only involves critical points that are not cusps, the form of  $\text{div}(r)$  in (3) works fine for our purpose.

Next we show  $\mathbb{Q}(r, u) = \mathbb{Q}(X_0(N))$  for the functions  $r, u$  in (1). First we prove a lemma.

**Lemma 2.4.** *Let  $N > 1$  be an integer and  $f \in S_2(\Gamma_0(N))$  be a newform. Suppose  $\alpha \in SL_2(\mathbb{Z})$  such that  $f|[\alpha] = f$ , then  $\alpha \in \Gamma_0(N)$ .*

*Proof.* Write  $\alpha = \begin{pmatrix} a & b \\ M & d \end{pmatrix}$ . First we show that it suffices to consider the case where  $d = 1$ . Since  $(M, d) = 1$ , there exists  $y, w \in \mathbb{Z}$  such that  $My + dw = 1$ . By replacing  $(y, w)$  with  $(y + kd, w - kM)$  if necessary, we may assume  $(y, N) = 1$ . So we can find  $x, z \in \mathbb{Z}$  such that  $\gamma = \begin{pmatrix} x & y \\ Nz & w \end{pmatrix} \in \Gamma_0(N)$ . Now  $\alpha\gamma = \begin{pmatrix} * & * \\ M & 1 \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$  and  $f|[\alpha\gamma] = f$ .

Let  $w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$  be the Fricke involution on  $X_0(N)$ . Then  $f|w_N = \pm f$ , hence  $f|w_N\alpha w_N = f$ . We compute that  $w_N\alpha w_N = \begin{pmatrix} -N & M \\ 0 & -N \end{pmatrix}$ , thus  $f(q) = f|[\begin{pmatrix} -N & M \\ 0 & -N \end{pmatrix}](q) = f(q\zeta_N^{-M})$ , where  $\zeta_N = e^{2\pi i/N}$ . The leading term of  $f(q)$  is  $q$ , while the leading term of  $f(q\zeta_N^{-M})$  is  $\zeta_N^{-M}q$ . So we must have  $\zeta_N^{-M} = 1$ , i.e.,  $N \mid M$ . Hence  $\alpha \in \Gamma_0(N)$  and the proof is complete.  $\square$

**Proposition 2.5.** *Let  $r, u$  be as defined in (1), then  $\mathbb{Q}(r, u) = \mathbb{Q}(X_0(N))$ .*

*Proof.* Consider the modular curve  $X(N)$  defined over the field  $K = \mathbb{Q}(\mu_N)$ . Its function field  $K(X(N))$  is a Galois extension of  $K(u)$  containing  $K(X_0(N))$ . It follows that the conjugates of  $r$  in the extension  $K(X(N))/K(u)$  are of the form  $r_i = r|[\alpha_i]$  where  $\{\alpha_i\}$  is a set of coset representatives of  $\Gamma_0(N) \backslash \text{SL}_2(\mathbb{Z})$ . Note that  $\mathbb{Q}(r, u) = \mathbb{Q}(X_0(N))$  if and only if the  $r_i$  are distinct. Suppose towards contradiction that there exists  $i \neq j$  such that  $r|[\alpha_i] = r|[\alpha_j]$ . Since  $j$  and  $j'$  are invariant under the action of  $\text{SL}_2(\mathbb{Z})$ , we see that  $f|[\alpha_i] = f|[\alpha_j]$ . Let  $\alpha = \alpha_i\alpha_j^{-1}$ , then  $\alpha \in \text{SL}_2(\mathbb{Z})$  and  $f|[\alpha] = f$ . So Lemma 2.4 implies  $\alpha \in \Gamma_0(N)$ , so  $\Gamma_0(N)\alpha_i = \Gamma_0(N)\alpha_j$ , a contradiction.  $\square$

**Lemma 2.6.** *Let  $g$  be the genus of  $X_0(N)$ . If  $T \geq 2g - 2$  is a positive integer, then  $rj^T$  and  $u$  satisfy the second condition of Proposition 2.2.*

*Proof.* Let  $r_1 = rj^T$ . When  $T \geq 2g - 2$ , the support of  $\text{div}_\infty(r_1)$  is the set of all cusps. Suppose  $\gcd(f_n, f_0) > 1$ . Let  $p(y)$  be an irreducible factor of  $\gcd(f_0, f_n)$ . Consider the valuation  $\text{ord}_p$  on the field  $K(y)$ . Since  $P$  is irreducible, there exists an integer  $i$  with  $0 < i < n$  such that  $p \nmid f_i$ . Thus the Newton polygon of  $P$  with respect to the valuation  $\text{ord}_p$  has at least one edge with negative slope and one edge with positive slope. Therefore, for any Galois extension  $L$  of  $K(u)$  containing  $K(r, u)$  and a valuation  $\text{ord}_{\mathfrak{p}}$  on  $L$  extending  $\text{ord}_p$ , there exists two conjugates  $r', r''$  of  $r$  such that  $\text{ord}_{\mathfrak{p}}(r') < 0$  and  $\text{ord}_{\mathfrak{p}}(r'') > 0$ . This implies that  $\text{div}_0(r') \cap \text{div}_\infty(r'') \neq \emptyset$ . Fix  $L = K(X(N))$ , then all conjugates of  $r_1$  in  $K(X(N))/K(u)$  are of the form  $r_1(\alpha z)$  for some  $\alpha \in \text{SL}_2(\mathbb{Z})$ . Hence the set of poles of any conjugate of  $r_1$  is the set of all cusps on  $X(N)$ , a contradiction.  $\square$

Note that for any  $T \in \mathbb{Z}$ , we have  $\mathbb{Q}(rj^T, u) = \mathbb{Q}(r, u) = \mathbb{Q}(X_0(N))$ . Hence when  $T \geq 2g - 2$ , the pair  $(rj^T, u)$  satisfies both assumptions of Proposition 2.2. We thus obtain

**Theorem 2.7.** *Let  $T \geq 2g - 2$  be a positive integer and let  $P(x, y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$  be a minimal polynomial relation of  $rj^T$  and  $u$ . Then there exist integers  $A, B$  and a nonzero constant  $c$  such that*

$$F_{E,j}(y) = cf_0(1/y) \cdot y^A (y - 1728)^B.$$

*The integers  $A$  and  $B$  are defined as follows. Let  $\epsilon_i(N) = |\mathcal{E}_i(N)|$  for  $i = 2$  or  $3$  and let  $d_N = [\text{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$ , then  $A = \deg f_n - T \cdot d_N - \frac{1}{3}(d_N + 2\epsilon_3(N))$ ,  $B = -\frac{1}{2}(d_N + \epsilon_2(N))$ .*

*Proof.* Write  $\text{div}(\omega) = \sum n_z[z]$ . Applying Proposition 2.2 to  $rj^T$  and  $u$ , we get

$$(a) \quad \prod_{z: u(z) \neq 0, \infty} (y - u(z))^{n_z} \cdot (y - 1/1728)^{\frac{1}{2}(d_N + \epsilon_2(N))} = cf_0(y)$$

and

$$(b) \quad \sum_{z: u(z) = \infty} \text{ord}_z(\omega) + T \cdot d_N + \frac{1}{3}(d_N + 2\epsilon_3(N)) = \deg f_n - \deg f_0.$$

To change from  $u$  to  $j$ , we replace  $y$  by  $1/y$  in (a) and multiply both sides by  $y^{\deg f_0}$  to obtain

$$\prod_{z: j(z) \neq 0, \infty} (y - j(z))^{n_z} \cdot (y - 1728)^{\frac{1}{2}(d_N + \epsilon_2(N))} = cf_0(1/y)y^{\deg f_0}.$$

The contribution of  $\{z \in \text{div}(\omega) : j(z) = 0\}$  to  $F_{E,j}$  can be computed from (b), so

$$\begin{aligned} F_{E,j}(y) &= c \cdot y^{\deg f_n - \deg f_0 - T \cdot d_N - \frac{1}{3}(d_N + 2\epsilon_3(N))} y^{\deg f_0} \cdot (y - 1728)^{-\frac{1}{2}(d_N + \epsilon_2(N))} f_0(1/y) \\ &= c \cdot y^{\deg f_n - T \cdot d_N - \frac{1}{3}(d_N + 2\epsilon_3(N))} (y - 1728)^{-\frac{1}{2}(d_N + \epsilon_2(N))} f_0(1/y). \end{aligned}$$

□

Now we describe the algorithm *Poly Relation*.

---

**Algorithm 1** *Poly relation*


---

Input:  $E$  = Elliptic Curve over  $\mathbb{Q}$ ;  $N$  = conductor of  $E$ ;  $f$  = the newform attached to  $E$ ;  $g = g(X_0(N))$ ,  $d_N, \epsilon_2(N), \epsilon_3(N)$ , and  $c_N$  = number of cusps of  $X_0(N)$ .

Output: The critical  $j$ -polynomial  $F_{E,j}(x)$ .

- 1: Fix a large integer  $M$ .  $T := 2g - 2$ .
  - 2:  $r_1 := j^{2g-1}(j - 1728) \frac{f}{j^T}$ ,  $u := \frac{1}{j}$ .
  - 3:  $\deg r_1 := (2g - 1)d_N - c_N$ ,  $\deg u := d_N$ .
  - 4: Compute the  $q$ -expansions of  $r_1$  and  $u$  to  $q^M$ .
  - 5: Let  $\{c_{a,b}\}_{0 \leq a \leq \deg u, 0 \leq b \leq \deg r_1}$  be unknowns, compute a vector that spans the one-dimensional vector space  $K = \{(c_{a,b}) : \sum c_{a,b} r(q)^a u(q)^b \equiv 0 \pmod{q^M}\}$ .
  - 6:  $P(x, y) := \sum c_{a,b} x^a y^b$ . Write  $P(x, y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$ .
  - 7:  $A := \deg f_n - T \cdot d_N - \frac{1}{3}(d_N + 2\epsilon_3(N))$ ,  $B := -\frac{1}{2}(d_N + \epsilon_2(N))$ .
  - 8: Output  $F_{E,j}(x) = c f_0(1/x) \cdot x^A (x - 1728)^B$ .
- 

An upper bound on the number of terms  $M$  in the above algorithm can be taken to be  $2 \deg r \deg u + 1$ , by the following lemma.

**Lemma 2.8.** *Let  $r, u \in \mathbb{Q}(X_0(N))$  be non-constant functions. If there is a polynomial  $P \in \mathbb{Q}[x, y]$  such that  $\deg_x P \leq \deg u$ ,  $\deg_y P \leq \deg r$ , and*

$$P(r, u) \equiv 0 \pmod{q^M}$$

*for some  $M > 2 \deg u \deg r$ , then  $P(r, u) = 0$ .*

*Proof.* Suppose  $P(r, u)$  is non-constant as a rational function on  $X_0(N)$ , then  $\deg P(r, u) \leq \deg r^{\deg u} u^{\deg r} = 2 \deg u \deg r$ . It follows from  $P(r, u) \equiv 0 \pmod{q^M}$  that  $\text{ord}_{[\infty]} P(r, u) \geq M$ . Since  $M > 2 \deg u \deg r$ , the number of zeros of  $P(r, u)$  is greater than its number of poles, a contradiction. Thus  $P(r, u)$  is a constant function. But then  $P(r, u)$  must be 0 since it has a zero at  $[\infty]$ . This completes the proof. □

*Remark 2.9.* When  $N$  is square free, there is a faster method that computes  $F_{E,j}$  by computing the *Norm* of the modular form  $f$ , defined as  $\text{Norm}(f) = \prod f[[A_i]]$ , where  $\{A_i\}$  is a set of right coset representatives of  $\Gamma_0(N)$  in  $\text{SL}_2(\mathbb{Z})$ . This approach is inspired by Ahlrgen and Ono [1], where  $j$ -polynomials of Weierstrass points on  $X_0(p)$  are computed for  $p$  a prime.

*Remark 2.10.* Also for the sake of speed, instead of taking  $T = 2g - 2$  in the algorithm, we may take  $T = 0$ . First, if  $\text{div}(\omega)$  does not contain cusps (for example, this happens if  $N$  is square free), then the functions  $r$  and  $u$  already satisfies the assumptions of Proposition 2.2. Second, if  $\text{div}(\omega)$  does contain cusps, then  $\deg(r)$  will be smaller than its set value in the algorithm, due to cancellation between zeros and poles. As a result, the vector space  $K$  will have dimension greater than 1. Nonetheless, using a basis of  $K$ , we could construct a set of polynomials  $P_i(x, y)$  with  $P_i(r, u) = 0$ . Now  $P(x, y)$  is the greatest common divisor of the  $P_i(x, y)$ .

We show a table of critical  $j$ -polynomials. Recall that  $H_d(x)$  denotes the Hilbert class polynomial associated to a negative discriminant  $d$ . We use Cremona's labels for elliptic curves in Table 1.

---

<sup>1</sup>In this case  $\text{div}(\omega) = [1/4] + [3/4] + [1/12] + [7/12]$  in supported on cusps.

TABLE 1. Critical polynomials for some elliptic curves with conductor smaller than 100

$E$	$g(X_0(N))$	Factorization of $F_{E,j}(x)$
37a	2	$H_{-148}(x)$
37b	2	$H_{-16}(x)^2$
44a	4	$H_{-44}(x)^2$
48a	3	$1^1$
67a	5	$x^8 + 1467499520383590415545083053760x^7 + \dots$
89a	7	$H_{-356}(x)$

### 3. YANG PAIRS AND THE ALGORITHM *Poly Relation-YP*

The main issue with the algorithm *Poly Relation* is efficiency. The matrix we used to solve for  $\{c_{a,b}\}$  has size roughly the conductor  $N$ . As  $N$  gets around  $10^3$ , computing the matrix kernel becomes time-consuming. So a new method is needed.

We introduce an algorithm *Poly Relation-YP* to compute critical polynomials attached to elliptic curves. The algorithm is inspired by an idea of Yifan Yang in [11]. The algorithm *Poly Relation-YP* does not compute the critical  $j$ -polynomial. Instead, it computes a critical  $h$ -polynomial, where  $h$  is some modular function on  $X_0(N)$  chosen within the algorithm. First we restate a lemma of Yang.

**Lemma 3.1** (Yang [11]). *Suppose  $g, h$  are modular functions on  $X_0(N)$  with a unique pole of order  $m, n$  at the cusp  $[\infty]$ , respectively, such that  $\gcd(m, n) = 1$ . Then*

(1)  $\mathbb{Q}(g, h) = \mathbb{Q}(X_0(N))$ .

(2) *If the leading Fourier coefficients of  $g$  and  $h$  are both 1, then there is a minimal polynomial relation between  $g$  and  $h$  of form*

$$(4) \quad y^m - x^n + \sum_{a,b \geq 0, am+bn < mn} c_{a,b} x^a y^b.$$

Two non-constant modular functions on  $X_0(N)$  are said to be a *Yang pair* if they satisfy the assumptions of Lemma 3.1. Following [11], we remark that in order to find a minimal polynomial relation of a Yang pair, we can compute the Fourier expansion of  $y^m - x^n$  and use products of form  $x^a y^b$  to cancel the pole at  $[\infty]$  until we reach zero. This approach is significantly faster than the method we used in *Poly Relation*, which finds a minimal polynomial relation of two arbitrary modular functions. This gain in speed is the main motivation of introducing *Poly Relation-YP*.

Let

$$\eta = q^{\frac{1}{24}} \prod_{n \geq 1} (1 - q^n)$$

be the Dedekind  $\eta$  function. For any positive integer  $d$ , define the function  $\eta_d$  as  $\eta_d(z) = \eta(dz)$ .

An  $\eta$ -product of level  $N$  is a function of the form

$$h(z) = \prod_{d|N} \eta_d(z)^{r_d}$$

where  $r_d \in \mathbb{Z}$  for all  $d | N$ .

The next theorem of Ligozat gives sufficient conditions for a  $\eta$ -product to be a modular function on  $X_0(N)$ .

**Lemma 3.2** (Ligozat's Criterion [8]). *Let  $h = \prod_{d|N} \eta_d(z)^{r_d}$  be an  $\eta$ -product of level  $N$ . Assume the following:*

(1)  $\sum_d r_d \frac{N}{d} \equiv 0 \pmod{24}$ ; (2)  $\sum_d r_d d \equiv 0 \pmod{24}$ ; (3)  $\sum_d r_d = 0$ ; (4)  $\prod_{d|N} (\frac{N}{d})^{r_d} \in \mathbb{Q}^2$ .

*Then  $h$  is a modular function on  $X_0(N)$ .*

If  $h \in \mathbb{Q}(X_0(N))$  is an  $\eta$ -product, then it is a fact that the divisor  $\text{div}(h)$  is supported on the cusps of  $X_0(N)$ . The next theorem allows us to construct  $\eta$ -products with prescribed divisors.

**Lemma 3.3** (Ligozat [8]). *Let  $N > 1$  be an integer. For every positive divisor  $d \mid N$ , let  $(P_d)$  denote the sum of all cusps on  $X_0(N)$  of denominator  $d$ . Let  $\phi$  denote the Euler's totient function. Then there exists an explicitly computable  $\eta$ -product  $h \in \mathbb{Q}(X_0(N))$  such that*

$$\operatorname{div}(h) = m_d((P_d) - \phi(\gcd(d, N/d))[\infty])$$

for some positive integer  $m_d$ .

*Remark 3.4.* By ‘explicitly computable’ in Lemma 3.3, we mean that one can compute a set of integers  $\{r_d : d \mid N\}$  that defines the  $\eta$ -product  $h$  with desired property. It is a fact that the order of vanishing of an  $\eta$  product at any cusp of  $X_0(N)$  is a linear combination of the integers  $r_d$ . So prescribing the divisor of an  $\eta$ -product is equivalent to giving a linear system on the variables  $r_d$ . Thus we can solve for the  $r_d$ 's and obtain the  $q$ -expansion of  $h$  from the  $q$ -expansion of  $\eta$ .

**Proposition 3.5.** *Let  $D \geq 0$  be a divisor on  $X_0(N)$  such that  $D$  is supported on the cusps. Then there exists an explicitly computable  $\eta$ -product  $h \in \mathbb{Q}(X_0(N))$  such that  $\operatorname{div}(h)$  is of the form  $D' - m[\infty]$ , where  $m$  is a positive integer and  $D' \geq D$ .*

Recall our notation from section 2 that  $r = j(j - 1728)\frac{\omega}{dj}$ .

**Proposition 3.6.** *There exists an explicitly computable modular function  $h \in \mathbb{Q}(X_0(N))$  such that*

- (1) *The functions  $rh$  and  $j(j - 1728)h$  form a Yang pair;*
- (2)  *$j(j - 1728)h$  is zero at all cusps of  $X_0(N)$  except the cusp  $[\infty]$ .*

*Proof.* Let  $T = \operatorname{div}_\infty(j)$ . Note that the support of  $T$  is the set of all cusps. From (3) we have  $\operatorname{div}_\infty(r) \leq T$ ,  $\operatorname{div}(j(j - 1728)) = 2T$ ,  $\operatorname{ord}_{[\infty]}(T) = 1$ , and  $\operatorname{ord}_{[\infty]}(r) = 0$ . Applying Corollary 3.5 to the divisor  $D = 4(T - [\infty])$ , we obtain an  $\eta$ -product  $h \in \mathbb{Q}(X_0(N))$  such that  $\operatorname{div}(h) = D' - m[\infty]$ , where  $D' \geq D$ . Then  $\operatorname{div}_\infty(rh) = m[\infty]$  and  $\operatorname{div}_\infty(j(j - 1728)h) = (m + 2)[\infty]$ . If  $m$  is odd, then  $(m, m + 2) = 1$  and (1) follows. Otherwise, we can replace  $h$  by  $jh$ . Then a similar argument shows that  $rh$  and  $j(j - 1728)h$  have a unique pole at  $[\infty]$  and have degree  $m + 1$  and  $m + 3$ , respectively. Since  $m$  is even in this case, we have  $(m + 1, m + 3) = 1$  and (1) holds.

What we just showed is the existence of an  $\eta$ -product  $h \in \mathbb{Q}(X_0(N))$  s.t. either  $h$  or  $jh$  satisfies (1). Now (2) follows from the fact that  $\operatorname{div}_0(j(j - 1728)h) > 2(T - [\infty])$  and  $\operatorname{div}_0(j^2(j - 1728)h) > (T - [\infty])$ .  $\square$

Let  $h$  be a modular function that satisfies the conditions of Proposition 3.6. The next theorem allows us to compute  $F_{E, j(j-1728)h}(x)$ . For ease of notation, let  $\tilde{r} = rh$  and  $\tilde{h} = j(j - 1728)h$ .

**Theorem 3.7.** *Suppose  $h$  is a modular function on  $X_0(N)$  that satisfies the conditions in Corollary ???. Let  $P(x, y)$  be a minimal polynomial relation of  $\tilde{r}$  and  $\tilde{h}$  of form (4). Write  $P(x, y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$ , and let  $g$  be the genus of  $X_0(N)$ , then*

$$F_{E, \tilde{h}}(x) = x^{2g-2-\deg h} f_0(x).$$

*Proof.* The idea is to apply Proposition 2.2 to the Yang pair  $(\tilde{r}, \tilde{h})$ . By Lemma 3.1, every Yang pair satisfies the first assumption of Proposition 2.2. To see the second assumption holds, observe that  $f_n(y) = -1$  in (4), so  $\gcd(f_n(y), f_0(y)) = 1$ . Applying Proposition 2.2, we obtain

$$f_0(y) = \prod_{z \in \operatorname{div}_0(\tilde{r}) \setminus \operatorname{div}_\infty(\tilde{h})} (y - \tilde{h}(z))^{n_z}.$$

By construction of  $h$ , there is a divisor  $D \geq 0$  on  $X_0(N)$  supported on the finite set  $j^{-1}(\{0, 1728\}) \cup h^{-1}(0)$ , such that  $\operatorname{div}(rh) = \operatorname{div}(\omega) + D - (\deg h)[\infty]$ . Taking degrees on both sides shows  $\deg D = \deg h - (2g - 2)$ . Since  $\tilde{h}(z) = 0$  for all  $z \in \operatorname{supp} D$ , we obtain

$$f_0(x) = F_{E, \tilde{h}}(x) \cdot x^{\deg h - 2g + 2}.$$

This completes the proof.  $\square$

Next we describe the algorithm *Poly Relation-YP*.

**Algorithm 2** *Poly Relation-YP*

Input:  $E$  = Elliptic Curve over  $\mathbb{Q}$ ,  $f$  = the newform attached to  $E$ .

Output: a non-constant modular function  $h$  on  $X_0(N)$  and the critical  $\tilde{h}$ -polynomial  $F_{E,\tilde{h}}$ , where  $\tilde{h} = j(j-1728)h$ .

- 1: Find an  $\eta$  product  $h$  that satisfies Proposition 3.6.
- 2:  $\tilde{r} := j(j-1728)h_{\frac{f}{j}}$ ,  $\tilde{h} := j(j-1728)h$ .
- 3:  $M := (\deg \tilde{r} + 1)(\deg \tilde{h} + 1)$ .
- 4: Compute  $q$ -expansions of  $\tilde{r}$ ,  $\tilde{h}$  to  $q^M$ .
- 5: Compute a minimal polynomial relation  $P(x, y)$  of form (4) using the method mentioned after Lemma 3.1.
- 6: Output  $F_{E,\tilde{h}}(x) = x^{2g-2-\deg h} P(0, x)$ .

*Remark 3.8.* The functions  $\tilde{r}$  and  $\tilde{h}$  are constructed such that Theorem 3.7 has a nice and short statement. However, their degrees are large, which is not optimal for computational purposes. In practice, one can make different choices of two modular functions  $r$  and  $h$  with smaller degrees to speed up the computation. This idea is illustrated in the following example.

**Example 3.9.** Let  $E = \mathbf{664a1}$  with  $r_{\text{an}}(E) = 2$ . The genus  $g(X_0(664)) = 81$ . Let  $r_4$  be as defined in Remark 2.9. Using the method described in Remark 3.4, we found two  $\eta$ -products

$$h_1 = (\eta_2)^{-4}(\eta_4)^6(\eta_8)^4(\eta_{332})^6(\eta_{664})^{-12}, \quad h_2 = (\eta_2)^{-1}(\eta_4)(\eta_{166})^{-1}(\eta_8)^2(\eta_{332})^5(\eta_{664})^{-6}$$

with the following properties:  $h_1, h_2 \in \mathbb{Q}(X_0(N))$ ,  $\text{div}(rh_1) = \text{div}(\omega) + D - 247[\infty]$ , where  $D \geq 0$  is supported on cusps, and  $\text{div}(h_2) = 21[1/332] + 61[1/8] + 21[1/4] - 103[\infty]$ . Since  $(247, 103) = 1$ , the functions  $rh_1$  and  $h_2$  form a Yang pair. We then computed

$$F_{E,h_2}(x) = x^{160} - 14434914977155584439759730967653459200865032120265600267555196444x^{158} + \dots$$

The polynomial  $F_{E,h_2}$  is irreducible in  $\mathbb{Q}[x]$ .

#### 4. THE CRITICAL SUBGROUP $E_{\text{crit}}(\mathbb{Q})$

Recall the definition of the critical subgroup for an elliptic curve  $E/\mathbb{Q}$ :

$$E_{\text{crit}}(\mathbb{Q}) = \langle \text{tr}(\varphi(e)) : e \in \text{supp div}(\omega) \rangle.$$

Observe that to generate  $E_{\text{crit}}(\mathbb{Q})$ , it suffices to take one representative from each Galois orbit of  $\text{supp div}(\omega)$ . Therefore, if we let  $n_\omega$  denote the number of Galois orbits in  $\text{div}(\omega)$ , then

$$\text{rank}(E_{\text{crit}}(\mathbb{Q})) \leq n_\omega.$$

For any rational divisor  $D = \sum_{[z] \in X_0(N)} n_z[z]$  on  $X_0(N)$ , let  $p_D = \sum_{z \in \text{supp } D} n_z \varphi([z])$ , then  $p_D \in E(\mathbb{Q})$ . Note that  $p_D = 0$  if  $D$  is a principal divisor. The point  $p_{\text{div}(\omega)}$  is a linear combination of the defining generators of  $E_{\text{crit}}(\mathbb{Q})$ .

**Lemma 4.1.**  $6p_{\text{div}(\omega)} \equiv -3 \sum_{c \in \mathcal{E}_2(N)} \varphi(c) - 4 \sum_{d \in \mathcal{E}_3(N)} \varphi(d) \pmod{E(\mathbb{Q})_{\text{tors}}}.$

*Proof.* Let  $r_0 = \omega/dj$ , then  $r_0 \in \mathbb{Q}(X_0(N))$ , hence  $p_{\text{div}(r_0)} = 0$ . From  $\text{div}(r_0) = \text{div}(\omega) - \text{div}(dj)$ , we deduce that  $p_{\text{div}(\omega)} = p_{\text{div}(dj)}$ . The lemma then follows from the formula of  $\text{div}(dj)$  given in (2) and the fact that the image of any cusp under  $\varphi$  is torsion.  $\square$

**Proposition 4.2.** *Assume at least one of the following holds: (1)  $r_{\text{an}}(E) \geq 2$ . (2)  $X_0(N)$  has no elliptic point. Then  $\text{rank}(E_{\text{crit}}(\mathbb{Q})) \leq n_\omega - 1$ .*

*Proof.* By Lemma 4.1 and Theorem 1.3, either assumption implies that  $p_{\text{div}(\omega)}$  is torsion. But  $p_{\text{div}(\omega)}$  is a linear combination of the  $n_\omega$  generators of  $E_{\text{crit}}(\mathbb{Q})$ , so these generators are linearly dependent in  $E_{\text{crit}}(\mathbb{Q}) \otimes \mathbb{Q}$ . Hence the rank of  $E_{\text{crit}}(\mathbb{Q})$  is smaller than  $n_\omega$ .  $\square$



Now we are ready to prove Theorem 1.6.

**Proof of Theorem 1.6.** First, note that the definition of  $F_{E,j}$  only involves critical points that are not cusps. However, since images of cusps under  $\varphi$  are torsion, we can replace  $\text{div}(\omega)$  by  $\text{div}(\omega) \setminus \{\text{cusps of } X_0(N)\}$  if necessary and assume that  $\text{div}(\omega)$  does not contain cusps.

(1) Let  $d = \deg F_0$ , then there exists a Galois orbit in  $\text{div}(\omega)$  of size  $d$ , and the other  $(2g-2-d)$  points in  $\text{div}(\omega)$  are CM points. Let  $z$  be any one of the  $(2g-2-d)$  points, then  $j(z)$  is a root of  $H_{D_k}(x)$  and  $z \in \mathbb{Q}(\sqrt{D_k})$ . Since  $\text{div}(\omega)$  is invariant under the Fricke involution  $w_N$ , one sees that  $j(Nz)$  is also a root of  $F_{E,j}$ . Therefore,  $j(Nz)$  is the root of  $H_{D_{k'}}(x)$  for some  $1 \leq k' \leq m$ . Since  $z$  and  $Nz$  define the same quadratic field, we must have  $\mathbb{Q}(\sqrt{D_k}) = \mathbb{Q}(\sqrt{D_{k'}})$ , which implies  $k = k'$  by our assumption. It follows that  $[z]$  is a “generalized Heegner point” and  $\text{tr}(\varphi([z]))$  is torsion. By the form of  $F_{E,j}$ , there exists a point  $[z_0] \in \text{supp div}(\omega)$  such that  $j(z_0)$  is a root of  $F_0$ . Then we have  $\text{rank}(E_{\text{crit}}(\mathbb{Q})) = \text{rank}(\langle \text{tr}(\varphi([z_0])) \rangle) = \text{rank}(\langle p_{\text{div}(\omega)} \rangle)$ . Lemma 4.1 implies  $\langle p_{\text{div}(\omega)} \rangle = 0$ , and it follows that  $\text{rank}(E_{\text{crit}}(\mathbb{Q})) = 0$ .

(2) If  $F_{E,h}$  is irreducible, then we necessarily have  $n_\omega = 1$ , and the claim follows from Proposition 4.2.

*Remark 4.3.* Christophe Delaunay has an algorithm to compute  $\text{div}(\omega)$  numerically as equivalence classes of points in the upper half plane (see [5] and [6]). A table of critical points for  $E = \mathbf{389a}$  is presented in [5, Appendix B.1]. The results suggested that  $\text{div}(\omega)$  contains two Heegner points of discriminant 19, and the critical subgroup  $E_{\text{crit}}(\mathbb{Q})$  is torsion. Using the critical  $j$ -polynomial for  $\mathbf{389a}$  in Table 2, we confirm the numerical results of Delaunay.

## 5. DATA: CRITICAL POLYNOMIALS FOR RANK TWO ELLIPTIC CURVES

The columns of Table 2 are as follows. The column labeled  $E$  contains Cremona labels of elliptic curves, and those labeled  $g$  contains the genus of  $X_0(N)$ , where  $N$  is the conductor of  $E$ . The column labeled  $h$  contains a modular function on  $X_0(N)$ : either the  $j$  invariant or some  $\eta$ -product. The last column contains the factorization of the critical  $h$ -polynomial of  $E$  defined in Section 1.2. The factors of  $F_{E,j}$  that are Hilbert class polynomials are written out explicitly. Table 2 contains *all* elliptic curves with conductor  $N \leq 1000$  and rank 2. By observing that all the critical polynomials in the table satisfy one of the assumptions of Theorem 1.6, we obtain Corollary 1.7.

From our computation, it seems hard to find an elliptic curve  $E/\mathbb{Q}$  with  $r_{\text{an}}(E) \geq 2$  and  $\text{rank}(E_{\text{crit}}(\mathbb{Q})) > 0$ . Nonetheless, some interesting questions can be raised.

**Question 5.1.** For all elliptic curves  $E/\mathbb{Q}$ , does  $F_{E,j}$  always factor into a product of Hilbert class polynomials and one irreducible polynomial?

Yet another way to construct rational points on  $E$  is to take any cusp form  $g \in S_2(\Gamma_0(N), \mathbb{Z})$  and define  $E_g(\mathbb{Q}) = \langle \text{tr}(\varphi([z]) : [z] \in \text{supp div}(g(z)dz) \rangle$ .

**Question 5.2.** Does there exist  $g \in S_2(\Gamma_0(N), \mathbb{Z})$  such that  $E_g(\mathbb{Q})$  is non-torsion?

*Remark 5.3.* Consider the irreducible factors of  $F_{E,j}$  that are *not* Hilbert class polynomials. It turns out that their constant terms has many small primes factors, a property also enjoyed by Hilbert class polynomials. For example, consider the polynomial  $F_{\mathbf{67a},j}$ . It is irreducible and not a Hilbert class polynomial, while its constant term has factorization

$$2^{68} \cdot 3^2 \cdot 5^3 \cdot 23^6 \cdot 443^3 \cdot 186145963^3.$$

It is interesting to investigate the properties of these polynomials.

*Remark 5.4.* The polynomial relation  $P(x, y)$  between  $r$  and  $u$  can be applied to other computational problems regarding elliptic curves and modular forms. For example, one can use it to compute Fourier expansions of the newform  $f$  at every cusp (see [4]).

## REFERENCES

- [1] Scott Ahlgren and Ken Ono. Weierstrass points on  $X_0(p)$  and supersingular  $j$ -invariants. *Mathematische Annalen*, 325(2):355–368, 2003.
- [2] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over  $\mathbb{Q}$ : wild 3-adic exercises. *Journal of the American Mathematical Society*, pages 843–939, 2001.
- [3] Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein. Nonvanishing theorems for  $L$ -functions of modular forms and their derivatives. *Inventiones mathematicae*, 102(1):543–618, 1990.

TABLE 2. Critical polynomials for elliptic curves of rank 2 and conductor  $< 1000$ 

$E$	$g(X_0(N))$	$h$	Factorization of $F_{E,h}(x)$
389a	32	$j$	$H_{-19}(x)^2(x^{60} + \dots)$
433a	35	$j$	$x^{68} + \dots$
446d	55	$j$	$x^{108} + \dots$
563a	47	$j$	$H_{-43}(x)^2(x^{90} - \dots)$
571b	47	$j$	$H_{-67}(x)^2(x^{90} - \dots)$
643a	53	$j$	$H_{-19}(x)^2(x^{102} - \dots)$
664a	81	$\frac{\eta_4^2 \eta_8^5 \eta_{332}}{\eta_{166}^6 \eta_{664} \eta_2}$	$x^{160} - \dots$
655a	65	$j$	$x^{128} - \dots$
681c	75	$j$	$x^{148} - \dots$
707a	67	$j$	$x^{132} - \dots$
709a	58	$j$	$x^{114} - \dots$
718b	89	$j$	$H_{-52}(x)^2(x^{172} - \dots)$
794a	98	$j$	$H_{-4}(x)^2(x^{192} - \dots)$
817a	71	$j$	$x^{140} - \dots$
916c	113	$j$	$H_{-12}(x)^8(x^{216} + \dots)$
944e	115	$\frac{\eta_{16}^4 \eta_4^2}{\eta_8^6}$	$x^{224} - \dots$
997b	82	$j$	$H_{-27}(x)^2(x^{160} - \dots)$
997c	82	$j$	$x^{162} - \dots$

- [4] Hao Chen. Computing Fourier expansion of  $\Gamma_0(N)$  newforms at non-unitary cusps. In preparation.
- [5] Christophe Delaunay. Ph.D. thesis. 2002.
- [6] Christophe Delaunay. Critical and ramification points of the modular parametrization of an elliptic curve. 2005.
- [7] Benedict H Gross and Don B Zagier. Heegner points and derivatives of  $L$ -series. *Inventiones mathematicae*, 84(2):225–320, 1986.
- [8] Gérard Ligozat. Courbes modulaires de genre 1. *Mémoires de la Société Mathématique de France*, 43:5–80, 1975.
- [9] B. Mazur and P. Swinnerton-Dyer. Arithmetic of Weil curves. *Invent. Math.*, 25:1–61, 1974.
- [10] William Stein. *Algebraic number theory, a computational approach*. 2012.
- [11] Yifan Yang. Defining equations of modular curves. *Advances in Mathematics*, 204(2):481–508, 2006.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WASHINGTON, SEATTLE, WASHINGTON 98105  
*E-mail address*: `chenh123@uw.edu`